Background to the development of passkeys in the last few years

A Situation that the Security Services, App builders and others want to change:

The Increasingly sophisticated hacking of logins ***demands*** (at the least):

A long password containing numbers, symbols, capitals and unmemorable letters which should be changed occasionally
PLUS
2FA - ie another 6 digit code, often time limited, that is obtained from an authenticator (preferable) or via SMS text (not so safe).

This cumbersome system is often not followed or clients forget passwords and lock themselves out of important services, requiring call centre intervention.

Result The consumer internet operators got together and came up with FIDO 2 passkey system.

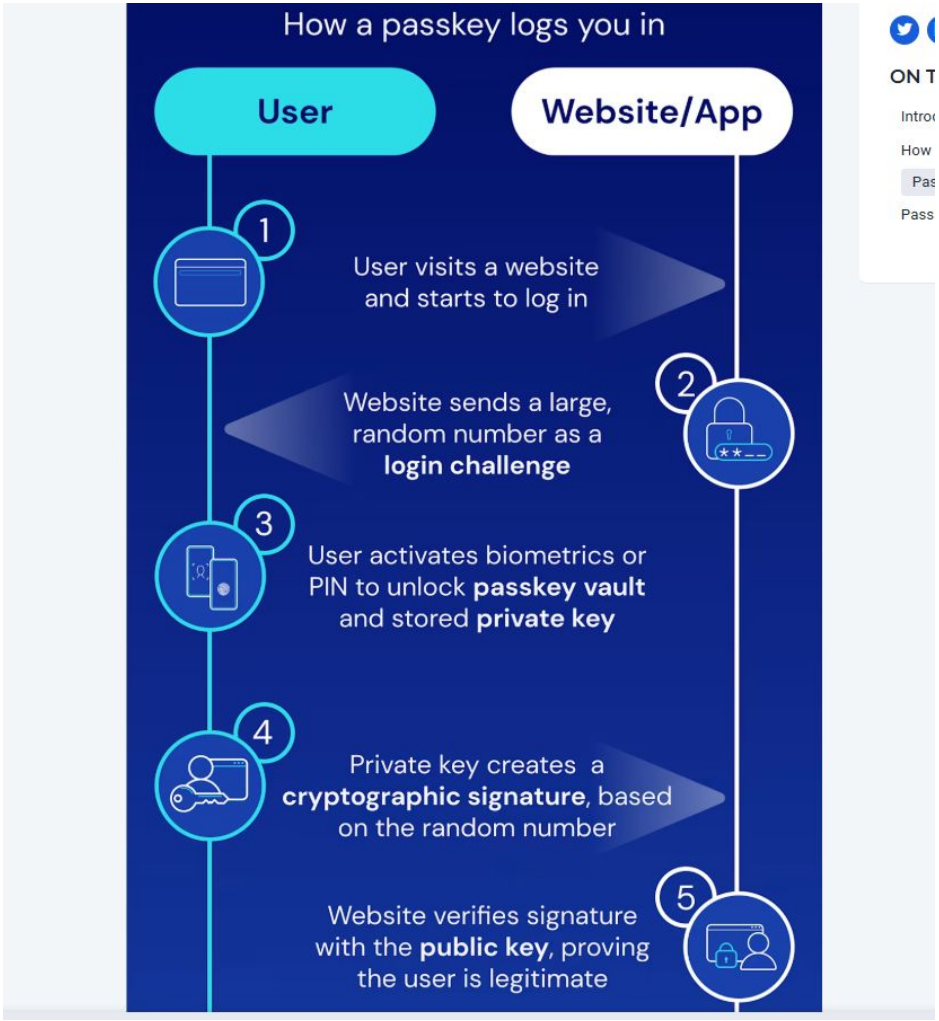
Taken from "Setting up a Paypal passkey - Q &A"

Unlike passwords, passkeys can only exist on your devices. They can't be written down or accidentally be given to a bad actor. When you use a passkey to sign in to your PayPal account, it proves to PayPal that you have access to your device and are able to unlock it. (ie "*Something you own and have nearby, plus something you know")*

If your device is lost or stolen, you can still log in to PayPal with your password or a one-time passcode.

Your PayPal account on the lost or stolen device cannot be accessed using the saved passkey without your face, fingerprint or PIN. As an extra precaution, you can also remove the passkey associated with the lost or stolen device.

When you create a passkey, it is ***saved to a password manager*** linked to your device. If you try to log in on a different device that is not connected to the same password manager or that is connected to a different password manager account (e.g. different iCloud account for iCloud keychain), you will not be able to use this passkey. You can create another passkey on this new device



Device specific - IMEI number…

but see also the role of password managers to allow a passkey to be used across devices.

Setting up a Passkey to an app - needs your permission and choice of passkey (biometric, in some cases abbreviated PIN or physical USB stick= Yubikey or similar)

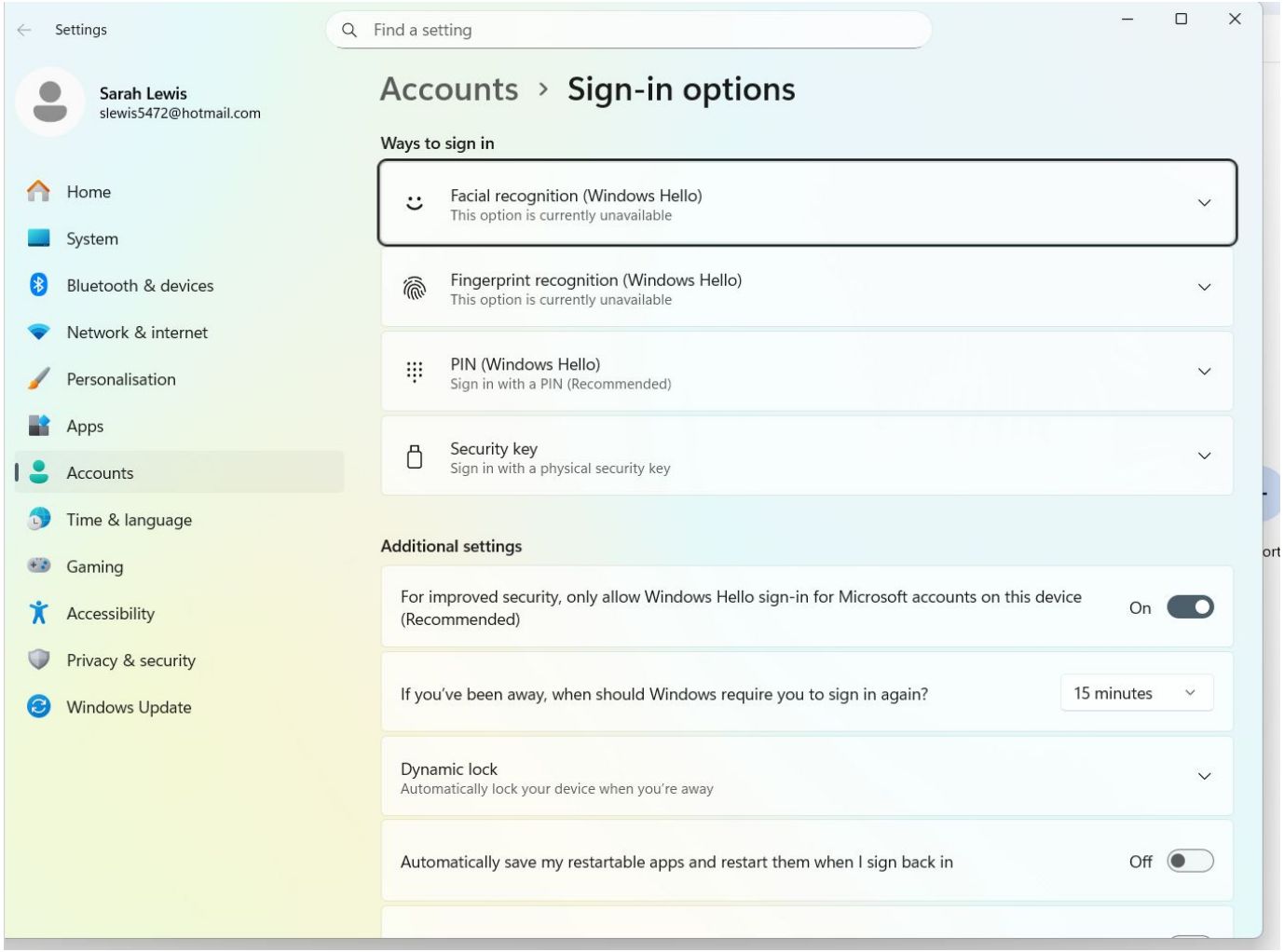
Behind the scenes - your browser, operating system, additional program (password managers), are used to generate the cryptographic exchange needed by:

The Public Key (from the app) sending a coded “question” ie login challenge.
Your Private key (on your device) asking for your Biometric/ key, then unlocking the response code.

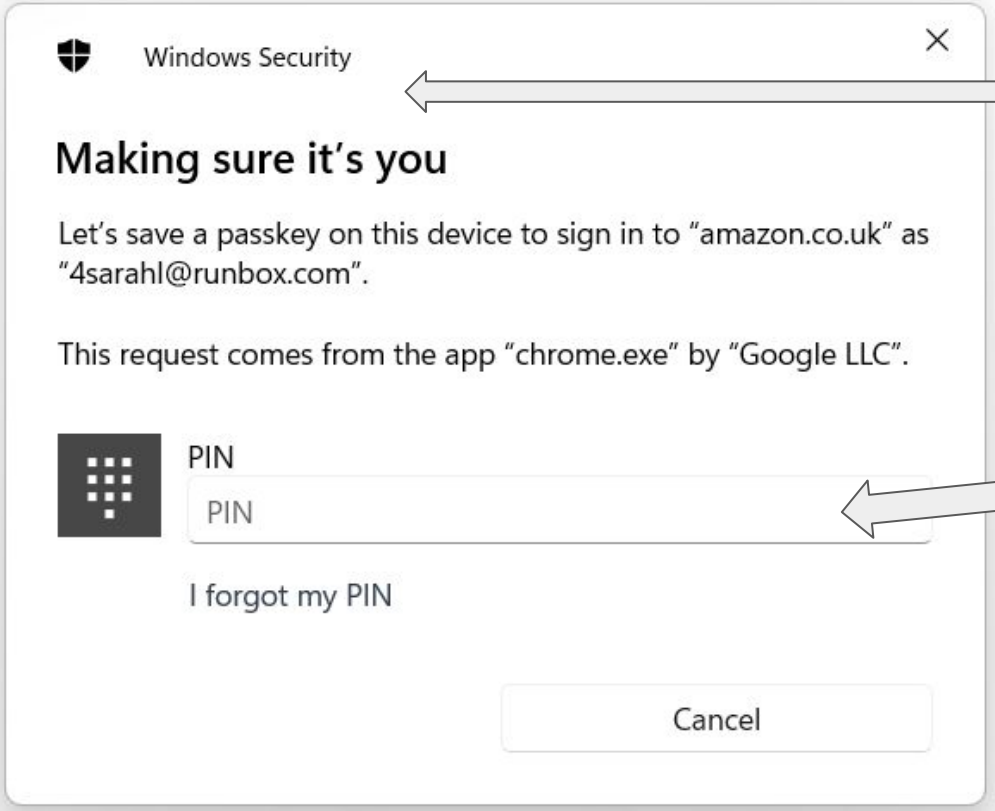
Device must be running a recent OS and up-to-date major browser

Only certain, well-funded apps have the FIDO capability to offer passkey login.

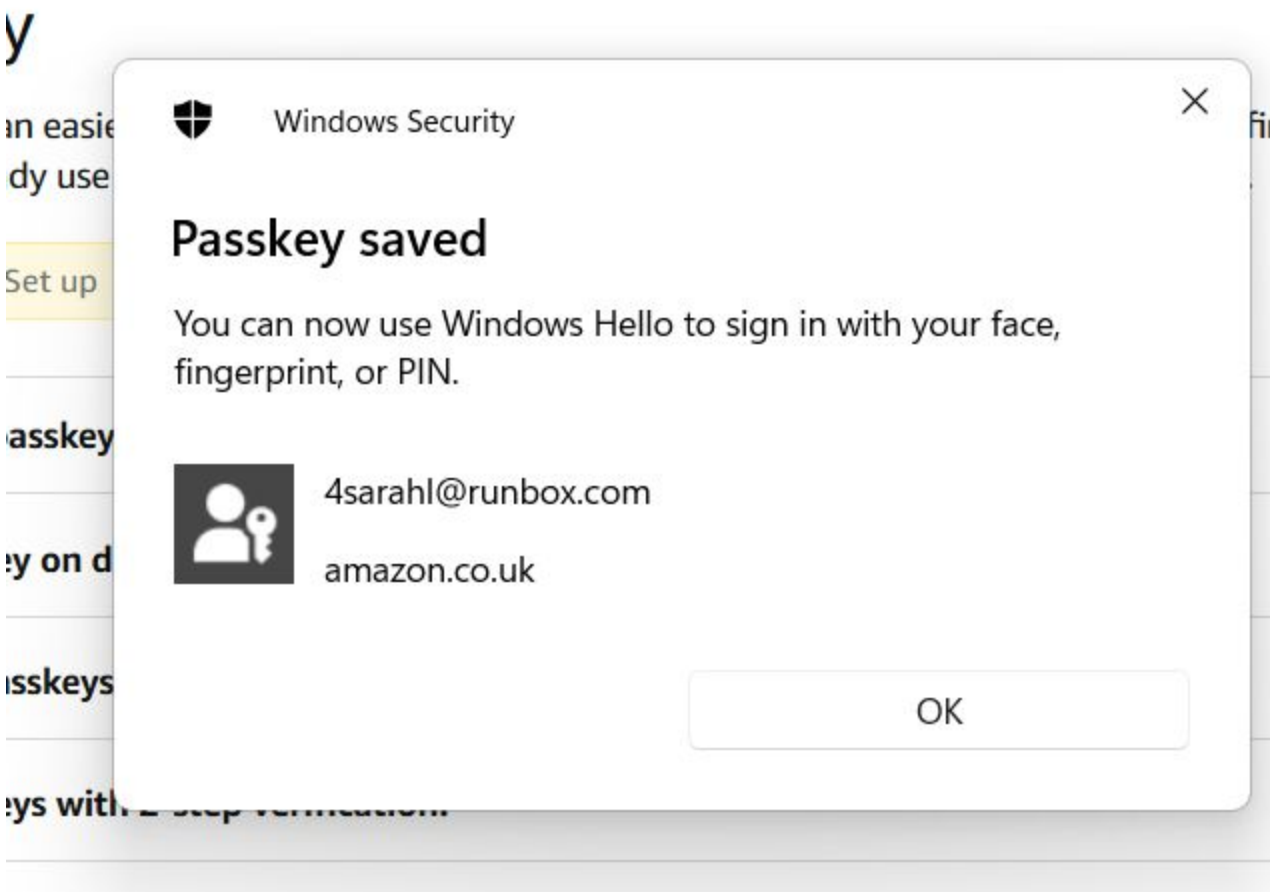
Everybody who owns a laptop or tablet/phone has at least one Passkey



Search “Windows Hello” on a Windows laptop brings up my only relevant passkey setting - to Windows login ie loading your Windows account on booting up.

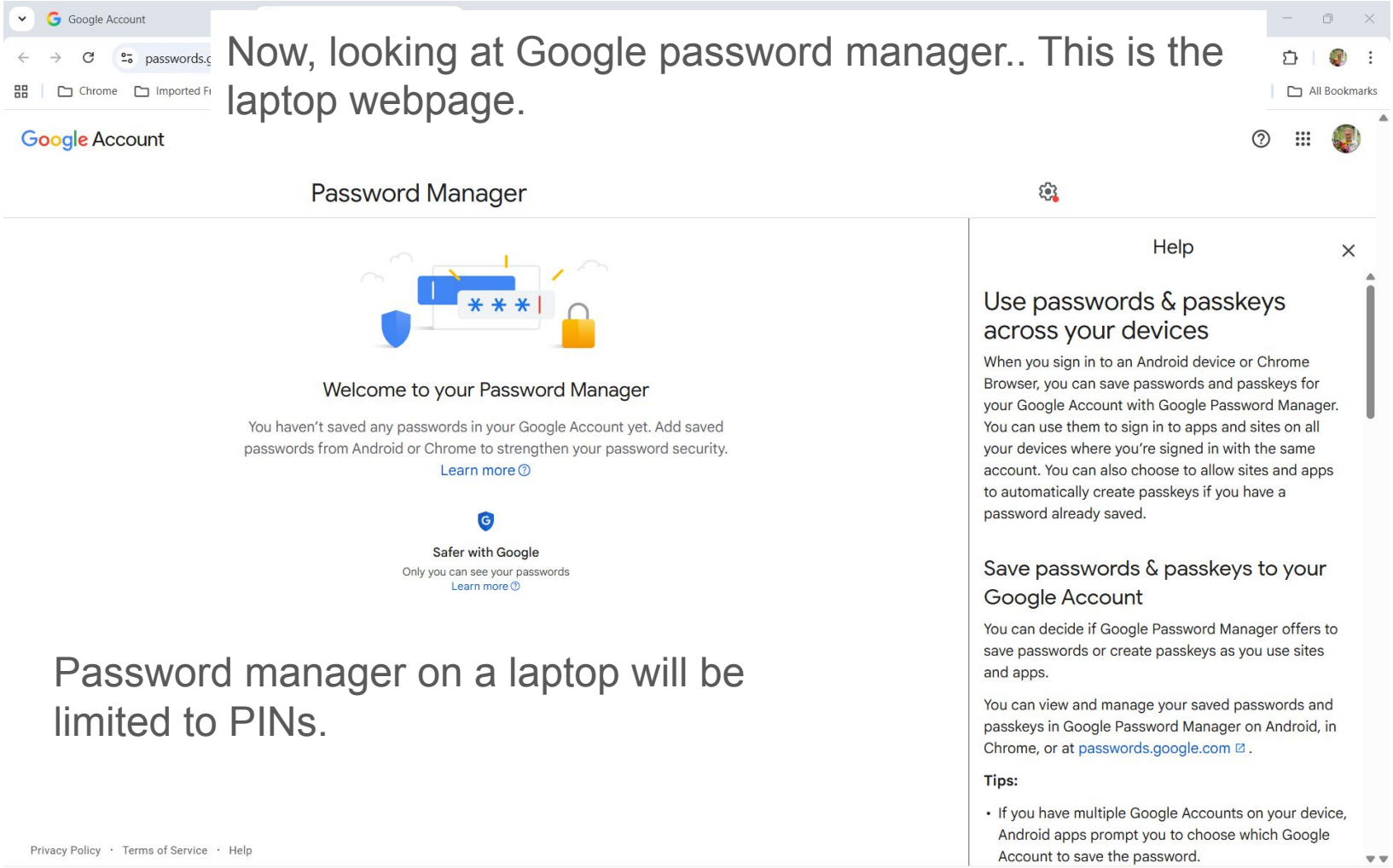


Trial passkey setup - on my Amazon account via MS laptop.
Windows software popup - asks for MS login PIN, which is itself a passkey!



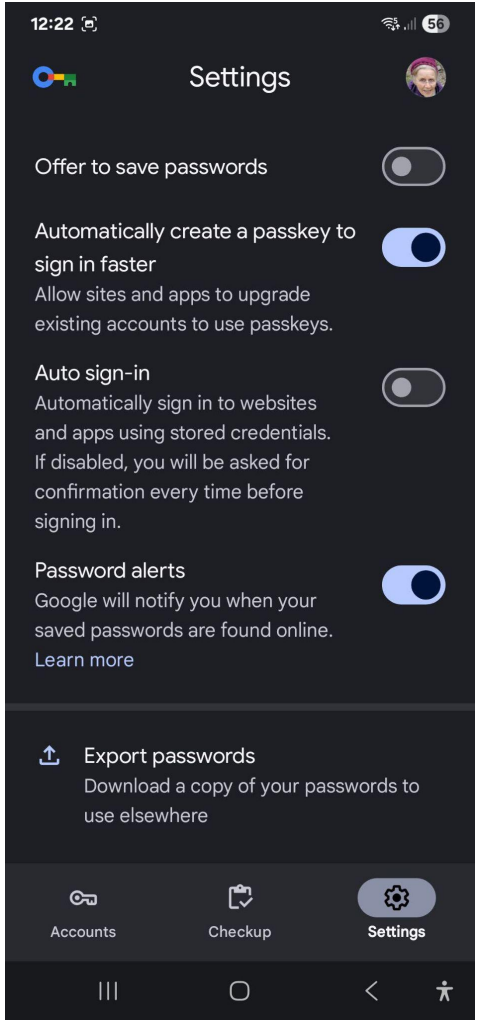
Windows Hello = Windows password manager

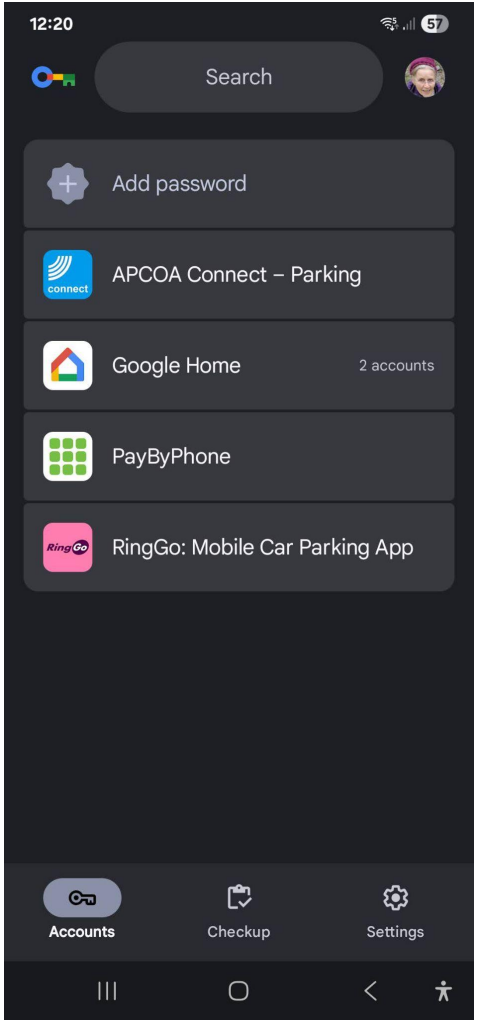
Now, looking at Google password manager.. This is the laptop webpage.



Password manager on a laptop will be limited to PINs.

On an Android device Google p’wd manager (my phone)





My few passkeys: mainly parking apps

Banks - a special case

Banking *apps* allow passkey ie biometric login - but occasionally ask you to use a longer 5 digit (or more) login number in addition. They only allow limited banking transactions eg not setting up new payees or change of account details.

Banking *websites* accessed from a laptop require the full works: 12 digit customer number (or full sortcode/account number etc) plus Mobile PINsEntry or PINsEntry device to generate a further bank-account-specific 8 digit PIN code *with each login.*

Only then are full banking activities offered.

At present, it is mainly the major purchasing apps (Amazon, eBay etc) and the operating system (email) accounts themselves (Microsoft online, Google, iCloud etc) that can offer passkeys, as the setup modifications to their websites for the codification, is expensive and intensive.

More apps will follow as hacking incidents increase...